# IoT Data Trustworthiness and Sentinels

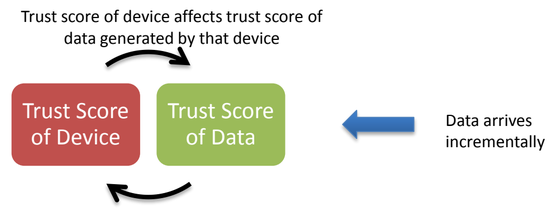
Stephen Adams and Peter Beling
University of Virginia

## NEED & INDUSTRIAL RELEVANCE

- Data is being collected at an ever increasing rate.
- Technological advances allow users to store and analyze the vast amounts of data present in modern society.
- The sources of data are diverse and include sensor networks, smart phones, cyber-physcial systems, and social networks.
- End users extract information from collected data and ultimately wish to make decisions utilizing this data.
- One common interest to several domains is the need to evaluate the trustworthiness of the data being collected and supplied to end users.
- Corrupted data, either intentionally corrupted or through natural causes, supplied to an end user or decision maker will degrade the performance of the system and could lead to incorrect or even fatal decisions.

## PROJECT GOALS

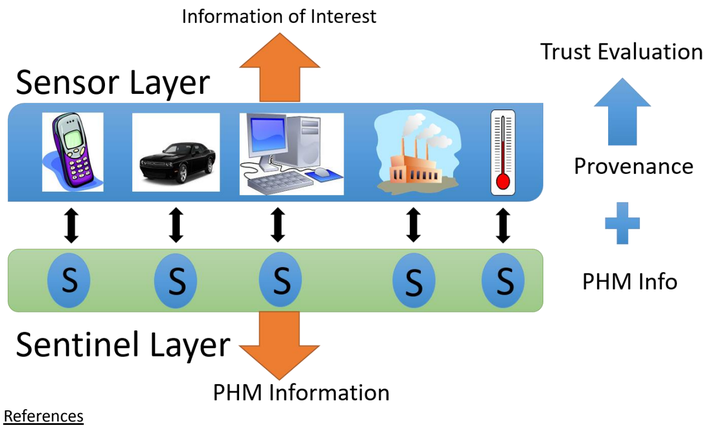
- Develop algorithmic approaches to evaluating the trustworthiness of data in large IoT networks
- Develop trust algorithm that are flexible and can be applied to several types of IoT networks
- Focus on the trust of individual pieces of data rather than trust of nodes in the network. However, these two notions of trust are inherently linked.[1]




## OBJECTIVES

- Literature review.
- Test existing models in the literature.
- Construct simulation of use cases.
- Develop new trust model or extend previous models to use case.
- Evaluate trade-offs of different models: scaling, power consumption, feature selection, resilience.
- Develop framework for a decision system that incorporates trust estimates.
- Online learning of trust.

## APPROACH (RESEARCH METHODS)



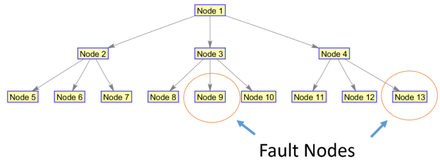

References
1. Bertino, Elisa. "Data Trustworthiness—Approaches and Research Challenges." *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*. Springer International Publishing, 2015. 17-25
2. Lim, Hyo-Sang, Yang-Sae Moon, and Elisa Bertino. "Provenance-based trustworthiness assessment in sensor networks." *Proceedings of the Seventh International Workshop on Data Management for Sensor Networks*. ACM, 2010.

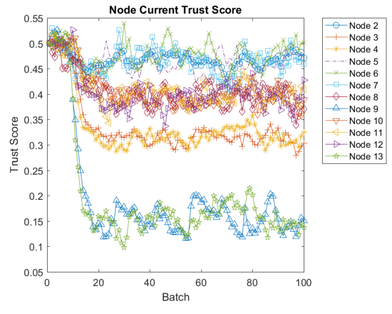
## DELIVERABLES/OUTCOMES

Year 1
- Literature review
- Code for existing models
- Code for new trust models
- Report including explanation of theory, simulation and testing results

Year 2
- Trade-off evaluation
- Decision system framework
- Online learning algorithms

Initial tests using Provenance-based model[2]




## IMPACT

- IoT sensor networks are growing and trust in the data being collected will be paramount to future decision systems that will rely on these networks. This project will provide the foundation for trust assessment in this area as well as contribute to the wider trust literature and research.
- Companies that utilize IoT networks will be provided with techniques for assessing the trust of their collected data. Further, a company could use the developed techniques in existing products or provide these services to customers.



*www.nsfcvdi.org*

VDI Center for Visual & Decision Informatics

*A National Science Foundation Industry/ University Cooperative Research Center*